2/5/23, 2:00 PM   MIP84: Activate Protocol-Owned Vault Emulation - Maker Improvement Proposals / Archive - The Maker Forum

Case 1:22-cv-08478-VSB   Document 30-23   Filed 02/14/23   Page 1 of 8

Welcome to the MakerDAO Forum! The following points will allow you to better understand governance and the forum.   ✕

Respectful and good-faith **discussion** should be the cornerstone of any decision-making process. In trying to enact change, please keep this principle in mind.

MakerDAO's **governance** has on-chain (**Voter Portal**) and off-chain (**Forum**) components. Community-driven discussions, well-reasoned arguments, and voting in this forum all have the ability to influence the Maker Protocol without the need for tokens. Here are some tips on navigating the forum:

---

ekryski   **Sep '22**

> rune:
>
> The only reason why there was an issue during black thursday was because of a very optimistic configuration of the auction parameters that performed badly in the selloff. The current liquidation system would have handled it flawlessly and Maker would have profited overall from black thursday.

> rune:
>
> Overall, while I think this has been iterated ad nauseam at this point, there is obviously financial risk in building up a large leveraged, staked ETH position. But it is justified by a much more significant risk posed by the bad trajectory crypto regulation is on following the crypto crash, terra and celsius collapse etc.

This is fair. The downside risk is certainly much lower if accumulation happens near bottom of a prolonged bear market as opposed to ATHs.

> psychonaut:
>
> Yeah, it looks like the EndGame is shaping up to be largely a referendum on whether the risk posed by bad crypto regulation is severe enough to justify moving most of our surplus buffer to a large leveraged, staked ETH position.

Agree. Seems to be shaping up this way.

> CodeKnight:
>
> Could @Risk-Core-Unit weigh in on roughly what they would consider a safe lower limit?

Skip to main content essimistic/optimistic models based on ETH/USD price and Maker's holdings as a % of total outstanding supply (with PoS we can fairly accurately model ETH

issuance rate).

If Maker accumulates too much ETH I think it could end up having adverse affects. As OlympusDAO found out, too much protocol owned liquidity for certain assets can actually kill usage.

---

rune   **Sep '22**

> psychonaut:
>
> Yeah, it looks like the EndGame is shaping up to be largely a referendum on whether the risk posed by bad crypto regulation is severe enough to justify moving most of our surplus buffer to a large leveraged, staked ETH position.

I don't think that's a good way to evaluate it, because it is not the biggest change introduced by the Endgame Plan, and by itself just accumulating ETH isn't gonna provide a meaningful solution to the long term problem of bad regulation.

In particular the MetaDAOs with their frontends, innovation potential etc and the significant tokenomics changes that they bring, including emissions of 60000 MKR per year to benefit the MetaDAO token liquidity, and the significant yield farming value this in turn provides to MKR holders and Maker users, is a more impactful change than the Protocol Owned Vault.

There's also the removal of MKR as an automatic backstop for Dai while enabling MKR as Dai collateral and using the tokenomics to accumulate massive amounts of captive liquidity for DAI, ETHD and MKR through Elixir.

By combining all of these elements together we get a much higher likelihood of an equilibrium that can survive even the absolute worst case scenario of regulatory overreach without losing critical mass for self sustainability.

---

rspa **Recognized Delegate**   **Sep '22**

> rune:
>
> Any Dai available in the Pause Proxy, whether from POVEDC or Starting Collateral, is used to accumulate Lido Staked ETH, and later EtherDai, using a DssKiln implementation sourcing liquidity from a liquid DEX. After the launch of Elixir, the DssKiln target will be the Elixir balancer pool.

Skip to main content

> • Buy: stETH

- `hop`: 20 minutes
- `lot`: 7000

If these parameters and some previous purchases are known, isn't there a very strong risk that arbitrageurs front run these purchases?

---

psychonaut Immunefi Security Core Unit Deputy Facilitator 🛡 🛡 🛡 🛡 🛡 🛡 🛡   **Sep '22**

> rune:
>
> By combining all of these elements together we get a much higher likelihood of an equilibrium that can survive even the absolute worst case scenario of regulatory overreach without losing critical mass for self sustainability.

The details of your full EndGame proposal are too complex for me to be able to reason about with confidence. Maybe that is the fault of my preference for simplicity or maybe I feel that way because your proposal actually is too complex for anybody to evaluated confidently. That is why I've focused on the current MIP Set. I do feel like MIP84 is simple enough to understand. What you want to do is invest in staked ETH using money generated by RWA. That could work if the markets cooperate and we get modestly lucky. On the other hand, it's much higher risk than the status quo. Our leveraged position could get wiped out. We could see a large loss from RWA that we struggle to cover.

The usual mathematical way to evaluate alternatives is to assign probabilities to all possible outcomes and then multiply the gains/losses by the probabilities. It's probably wrong, but for simplicity, let's assume that the gains/losses are equal under both scenarios. I wonder if my probabilities for the full EndGame plan look reasonable to you?

Status quo:

- legal problem: 2/100
- insolvency: 0.1/100
- human resource churn: 0.1/100

EndGame:

- legal problem: 1/100
- insolvency: 1/100
- human resource churn: 10/100

Given that no DAO/Org re/design can address the risk of an off-chain DenyList, I have a hard time seeing a way to obtain a dramatic reduction in potential legal problems. I'd like to understand in more concrete terms how the EndGame helps "survive even the absolute worst case scenario of

Skip to main content What is your attack model? How do you define *regulatory overreach* in specific and concrete terms? To me, the worst possible regulatory outcome would be:

1. Tornado Cash style OFAC sanction of the PauseProxy, DAI, and associated contracts meaning that US allies are prohibited from interaction with the Maker protocol
2. Lawsuits initiated by US Federal agencies against all US-based persons suspected of contributing to the Maker protocol

I don't see how the EndGame improves upon the status quo for either of these two attack vectors. There is basically no defense for (1). For (2), it seems like the only defense is for Maker protocol contributors to conceal their identity. Whether we're in the status quo or EndGame, it seems to me that contributors have an equal ability to be pseudonymous. So how does EndGame help? 🕵️

Moi   **Sep '22**

> psychonaut:
>
> Tornado Cash style OFAC sanction of the PauseProxy, DAI, and associated contracts meaning that US allies are prohibited from interaction with the Maker protocol

On some occasions, the commercial volume will not be associated with pro-American commercial partners, so a high caliber problem would not be possible, although here we can start another mission that would be to further expand commercial ties regardless of the political tone, remember that cryotocurrencies they are apolitical

---

psychonaut Immunefi Security Core Unit Deputy Facilitator 🛡️ 🛡️ 🛡️ 🛡️ 🛡️ 🛡️ 🛡️   **Sep '22**

> rune:
>
> we get a much higher likelihood of an equilibrium that can survive even the absolute worst case scenario of regulatory overreach

Hm, sounds a lot like the reassurance given by the founders of Ooki DAI, "By transferring control to a DAO, bZeroX's founders touted to bZeroX community members the operations would be enforcement-proof—allowing the Ooki DAO to violate the CEA and CFTC regulations with impunity, as alleged in the federal court action." ^

Skip to main content

Primoz Risk Core Unit Team   **Sep '22**

> CodeKnight:
>
> Could @Risk-Core-Unit weigh in on roughly what they would consider a safe lower limit?

At this moment **we estimate Capital at risk** measures approximately $6m due to high collateralization ratio and high protection score maintained by borrowers (addressing only non RWA part). This is less than 1% of debt collateralized by volatile crypto collateral at $930m right now. However, during the bull market in November lat year Capital at risk figure reached up to $150-$200m, while the "risky debt" at the top measured $5.6bn, implying a 2.5%-3.5% buffer. After all the stress testing of whales in the past year and successful liquidations we believe the safe long term surplus buffer ratio is closer to 1.5%-2.0%. This means a surplus buffer of minimum $15m to about $60m if ETH grows 3x from here and the profile of the borrowers doesn't change (assumes only organic growth of exposure due to higher prices, no new implementations).

I can see why holding some ETH in reserves would be beneficial, because it allows part of the surplus assets exposed to stETH to grow at the similar pace as Maker's riskier crypto collateral exposure. In the past we couldn't accumulate enough DAI in surplus from fees while the "risky debt" grew significantly.

Of course there is the downside to it as well; when ETH starts crashing, surplus would reduce in size as well. The trick is to maintain virtual price ceilings at levels that prevent buying excessive amounts of ETH during bull runs and vice versa. This of course won't be perfectly timed but I still think the benefits of having this ability to grow surplus buffer more proportionally along risky loanbook outweigh the downsides of it. Especially since the current surplus buffer coverage allows Maker to gain exposure towards ETH.

🔗 **Risk Core Unit Month in Review: September 2022**

🔗 **MIP84c10-SP1: Modify Emulated Surplus Buffer Upper Limit**

AstronautThis Governance (GovAlpha) Core Unit Team   **Sep '22**

> Primoz:
>
> The trick is to maintain virtual price ceilings at levels that prevent buying excessive amounts of ETH during bull runs and vice versa.

Regarding the vice versa part, @rune does it make sense to consider adding price floors as well to the MIP prevent us from "selling low" in case of a crazy market crash?

Skip to main content

psychonaut   Immunefi Security Core Unit Deputy Facilitator   🛡️ 🛡️ 🛡️ 🛡️ 🛡️ 🛡️ 🛡️   **Sep '22**

> Primoz:
>
> addressing only non RWA part

I'd like to emphasize that @Primoz was only writing in consideration of on-chain collateral. His impression is that loss reserves for RWA are partitioned into a separate bucket? I'd like to learn more about the loss reserves for RWA.

---

rune   **Sep '22**

Regulatory overreach, attack etc can all just be though of as a physical attack against any identifiable object in the real world that Maker relies on. There are basically two categories, actions against collateral, or actions against contributor, infrastructure, voters or even holders.

Physical resilience of collateral

To deal with the potential risk of attack against RWA The Protocol Owned Vault helps with reducing reliance on RWA. By itself it is not enough, but it helps as it synergizes well with the other main approaches, including incentivizing ETHD vaults, MKR generation, and Elixir accumulation. In the end it is likely impossible to remove all or most RWA exposure without also activating negative rates, and to make sure the negative rates are as low as possible (that is, less negative), we need to use every tool available - which includes using the protocol owned vault to generate decentralized Dai.

The Endgame Plan also defines a category of RWA referred to as Physically Resilient RWA - the definition of such RWA collateral is that its economic value cannot simply be seized through a legal system at will. The are two main approaches to achieve collateral that can be considered Physically Resilient:

1. The first is to use technology that allows Maker Governance to remotely brick and unbrick machines, making it possible to, in some cases, sell off the "keys" to such a machine even if it has been seized. An example of this would be the hypothetical drone cargo ship.

2. The second approach is to achieve sociopolitical saturation through marketing, adoption and lobbying in an independent democracy with rule of law to the point where any kind of unjust action taken against Maker RWA collateral could impact elections, making it politically impossible.

Skip to main content

The other major type of physical resilience is the ability to survive attacks against identifiable contributors, infrastructure or users and voters.

Infrastructure resilience

Resilience of infrastructure is achieved through a switch towards decentralized exchange based oracles for the main collateral types used by Maker Core in the Endgame: ETH, MKR and MetaDAO tokens. For smaller tokens supported by MetaDAO Lending Engines, the MetaDAOs themselves can operate and secure the oracle networks that power them, and can be face penalties for not following best practice, which could for instance be related to the location of an oracle node. In the end the MetaDAOs are the taking first loss with their own junior capital in case successful attacks happens against their oracles nodes.

Contributor resilience

Resilience of contributors requires full anonymity of the workforce. This will not possible to implement in the short run, but it can be slowly worked towards and normalized over time, while the risk of an imminent attack is low, as it remains today. Maker Core cannot itself handle a workforce of anons, since it is a major challenge to deal with the sybil and embezzlement risk it poses. But MetaDAOs are the ideal solution to this problem, since from Maker's perspective it makes no difference if the contributors in the MetaDAOs are anonymous or not, for Maker it is just an interaction with another DAO. This way the embezzlement risk of sybil abuse is pushed to the MetaDAOs who can then iterate and develop their own solutions and frameworks to handle the root of the problem, which is tools and processes that adequately measure results rather than rely on trust and relationships.

User and voter resilience

Resilience of users and voters are the final and most difficult step, and is only reasonable to do completely once all the other forms of resilience have been developed adequately. It requires a fully functional local and decentralized toolkit - in the Endgame plan the underlying system for this is called the Homefront

The Homefront will enable secure interaction with Maker, Dai, blockchains, defi etc. As a part of this it also enables voting in Maker Governance, and delegating to earn voter incentives. Additionally, it must support all critical communication and coordination needs for Maker Governance, MetaDAO Governance and more generally just for anyone who may be in need of secure communications or the target of repression.

The key tool that the Endgame Plan uses to make adoption of full stack decentralized tech realistic, is the MetaDAO token farming, which will require the Homefront to access. Each MetaDAO will develop and mod the Homefront to create its own unique (but equally secure) MetaDAO frontend, and its main business objective is to maximize adoption of this MetaDAO frontend as it is from its MetaDAO frontend userbase that it generates most or significant portions

Skip to main content

How does this compare with Ooki DAO

Maker have already long ago completed the same steps that Ooki DAO did, but that does not protect us from the trajectory of crypto regulation and enforcement that is in motion following the erasure of crypto goodwill due to Terra, Celsius etc

The only way to deal with these risks is to go all the way and achieve actual physical resilience across the board. We should expect that over time, any attack surface that remains will be attacked with full force and could be used to destroy the entire project. Most likely we are not facing such a situation in the short run, and in all cases it is not realistic for us to get prepared within a short amount of time. So we have to assume that we have several years available to take the necessary steps and in the medium term prepare to become a real and uncompromised decentralized finance protocol operated by a real and uncompromised decentralized autonomous organization.

---

psychonaut Immunefi Security Core Unit Deputy Facilitator 🛡 🛡 🛡 🛡 🛡 🛡 🛡   **Sep '22**

> rune:
>
> obviously trolling and deliberately misunderstanding and misrepresenting me at every turn

I'm not sure I'd characterize it that way. I'm pushing you to flesh out your proposal. I do appreciate you spelling out your positions in more detail.

- "switch towards decentralized exchange based oracles" – Seems like something that the Oracles CU is equipt handle.
- "full anonymity of the workforce" – Not sure why this is not feasible in the status quo. Who is @LongForWisdom ?
- "Homefront" – This is the first mention I've seen of Homefront. I searched the forums and it might be the first time you mentioned it? It sounds like a privacy tool, maybe something like the combination of PGP + Aztec?

These three goals (Infra, Contrib, & User resilience) seem equally worthwhile to pursue in the status quo or the EndGame. We are in *agreement*. At the same time, I'm not convinced that the EndGame offers much of a difference compared to the status quo. Which brings us back to MIP84/POVE, appropriate given the topic of the original post.

Here, I guess we can agree to disagree. In my judgment, the risks posed by regulation (incl. unknown risks) are not severe enough to justify moving most of our surplus buffer to a large leveraged, staked ETH position. Even if I agreed that Maker urgently needs to transition to away from RWA exposure, we can't possibly buy enough collateral (i.e. stETH) fast enough to make a practical difference. Suppose we obtain the rosy outcome of $100M/yr in profits (even after increasing the DAI Savings Rate). That just doesn't make much of a dent in the $5B worth of stablecoin exposure. Rune, with POVE, it feels like you are trying to put a square peg through a

Skip to main content